Indian Health Service Information Security Plan and Strategy FY2004 - FY2009

Rob McKinney

In Support of IHS Goals and Initiatives

- Providing a secure and trusted IT environment
- Enhancing the ability of the Nation’s healthcare system to effectively respond to bioterrorism and other public health challenges
- Achieving excellence in IT management practices

Mission Statement

- ***Provide an agency-wide secure and trusted information technology environment in support of IHS' commitment, in partnership with American Indian and Alaska Native people, to raising their physical, mental, social, and spiritual health to the highest level.***

Vision

- *Develop and institutionalize an information security program that:*
  - *Promotes agency-wide security awareness and compliance*
  - *Facilitates collaboration and encourages partnership among Agency entities in development and support of information security requirements*
  - *Helps security personnel understand and implement information security policies and procedures*
  - *Encourages performance measurement and improvement*

Goals

- *1 – Improve the overall information security posture to adequately assure the confidentiality, integrity, and availability of information and information resources*
- *2 – Create an environment where all employees' actions reflect the importance of information security*
- *3 – Establish and maintain consistent agency-wide policies and procedures to protect IHS' information and information systems from abuse and inappropriate use*
- *4 – Ensure minimum security standards agency wide, consistent with Federal guidelines and best practices*
- *5 – Support integration of information security into IHS lines of business*
- *6 – Establish program metrics to measure information security program performance*

Objectives

- *Goal 1 – Improve the overall information security posture to adequately assure the [illegible] availability of information resources*

1.8 – Implement agency-wide use of Federal [illegible] (PKI)

1. [illegible]

Information Security Management [illegible] (ISMA) Plan of Action and Milestones (POA&M) process and tool

[illegible] Accreditation (C&A) for every major application (MA) and general support system (GSS)

Objectives

- *Goal 2 – Create an environment where all employees' actions reflect the importance of information security*

2.1 – All users receive information security awareness training

2.2 – Provide role-based training

Objectives

- *Goal 3 – Establish and maintain consistent agency-wide policies and procedures to protect IHS' information and information systems from abuse and inappropriate use*

3.[illegible] – [illegible] comply

[illegible] of

[illegible] disseminate

Objectives

- *Goal 4 – Ensure minimum security standards agency wide, consistent with Federal guidelines and best practices*

4.1 – Promote cooperation and coordination with IHS personnel in development and maintenance of standard hardware and software components and configurations

4.2 – Establish a capability to develop, document, validate, and disseminate standard hardware and software components and configurations in accordance with NIST and other federal guidelines

Objectives

- *Goal 5 – Support integration of information security into IHS lines of business*

5.1 – Accurately identify information security funding requirements to ensure that budget requests are responsive to information security priorities

5.2 – Ensure IT investment has a documented plan for addressing security at each stage in the investment lifecycle, including incorporation of security into current IT capital plans

Objectives

- *Goal 6 – Establish program metrics to measure information security program performance*

6.1 – Define measurable program [illegible] and establish metrics

6.2 – Develop, apply, and [illegible] action plans [illegible] progress results

Objectives

- *1.1 – Complete and maintain National Institute of Standards and Technology (NIST) Certification and Accreditation (C&A) for every major application (MA) and general support system (GSS)*
- *1.2 – Achieve and maintain Health Insurance Portability and Accountability Act (HIPAA) Security Rule compliance*
- *1.3 – Complete and maintain Privacy Impact Assessments (PIAs) for every MA and GSS*
- *1.4 – Ensure information systems are adequately protected*
- *1.5 – Implement HHS' Public-Key Infrastructure (PKI) initiative across IHS*
- *1.6 – Complete and maintain E-Authentication requirements*
- *1.7 – Develop an IHS Incident Response capability*
- *1.8 – Implement agency wide use of Federal Information Security Management Act (FISMA) Plan of Action and Milestones (POA&M) Process and tool*
- *1.9 – Implement an automated patch management system agency wide*

Objectives

- *2.1 – All users receive information security awareness training*
- *2.2 – Provide role-based training*

Objectives

- *3.1 – Update information security policies to comply with NIST standards and all applicable federal requirements*
- *3.2 – Develop agency-wide information security procedures to comply with NIST standards and all applicable federal requirements and disseminate*
- *3.3 – Promote implementation of agency-wide policies and procedures at all levels of IHS*
- *3.4 – Promote cooperation and coordination with Area personnel in development and maintenance of agency-wide policies and procedures*

Objectives

- *4.1 – Establish a capability to develop, document, validate, and disseminate standard hardware and software components and configurations in accordance with NIST and other federal guidelines*
- *4.2 – Promote cooperation and coordination with IHS personnel in development and maintenance of standard hardware and software components and configurations*

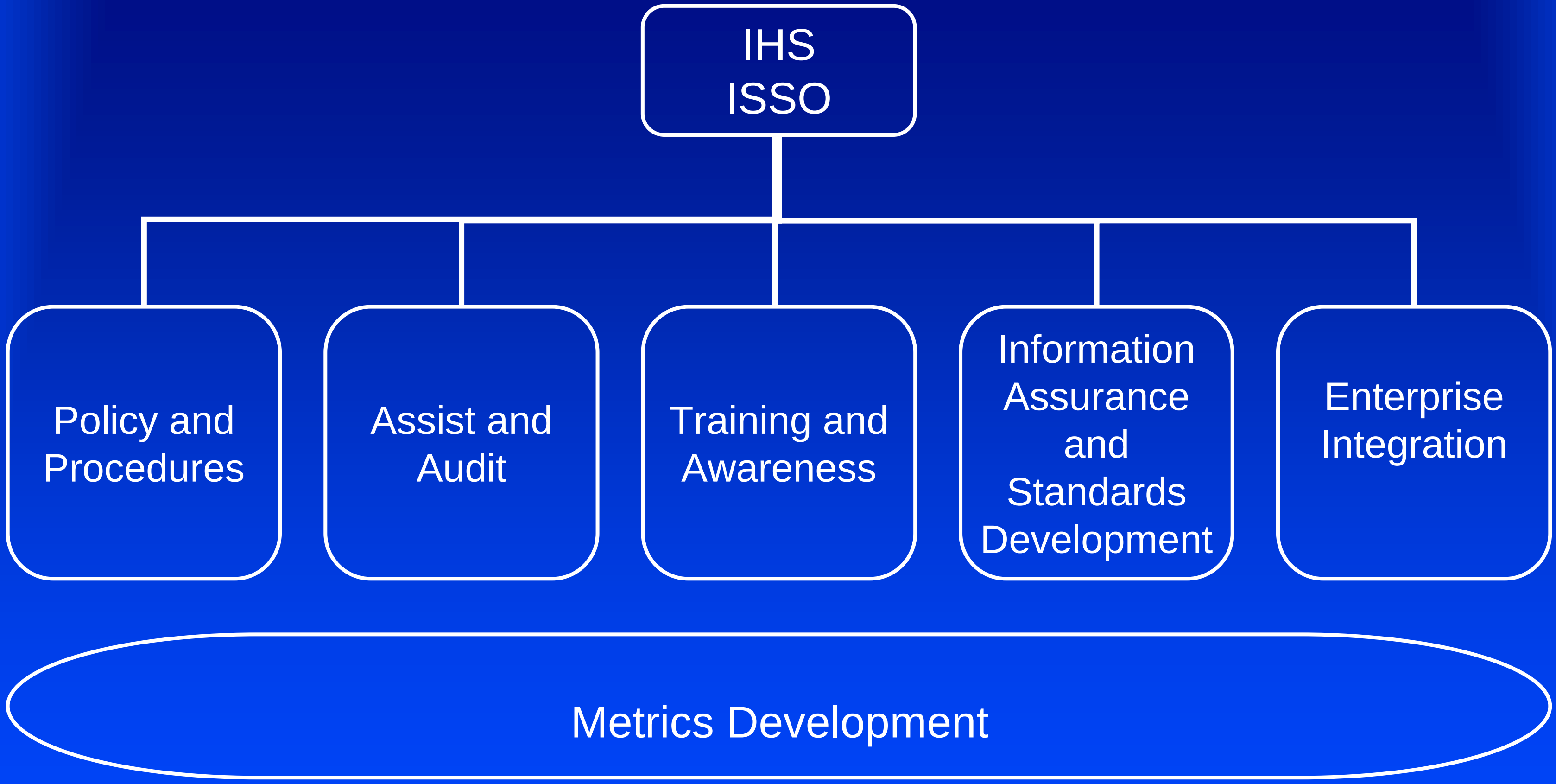
Objectives

- ***5.1 – Ensure IT investment has a documented plan for addressing security at each stage in the investment lifecycle, including incorporation of security into current IT capital plans***
- ***5.2 – Accurately identify information security funding requirements to ensure that budget requests are responsive to information security priorities***

Objectives

- *6.1 – Define measurable program results and establish metrics*
- *6.2 – Periodically apply metrics to determine progress*
- *6.3 – Develop or modify, and implement action plans according to progress results*

Functional Areas



IHS ISSO

Policy and Procedures

Assist and Audit

Training and Awareness

Information Assurance and Standards Development

Enterprise Integration

Metrics Development

Functional Area Descriptions

Policy and Procedures

Draft, coordinate, and disseminate policies and procedures in support of the IHS Information Security Program

Assist and Audit

Assist IHS facilities' information security efforts and Audit IHS facilities for compliance with information security program and system plans, policies, procedures, and standards

Training and Awareness

Provide data collection and instructional services, produce and implement information security and IT training and awareness products

Information Assurance and Standards Development

Track and provide information security advisories and recommendations, track and maintain system inventories, track and disseminate information security requirements, develop and issue software and hardware information security related configuration standards

Enterprise Integration

Provide support and facilitate integration of information security into enterprise initiatives

Policies and Procedures

- Conduct policy and procedure assessment activities
  - Policy identification and baseline, including IHS policies and handbook review and Area policies and procedures review
  - Conduct policy GAP analysis
  - Review policy infrastructure
  - Analyze internal interdependencies
  - Analyze external interdependencies
  - Develop Policies and Procedures performance measures
- Conduct policy and procedures performance activities
  - Develop Policies and Procedures document management
  - Revise handbooks
  - Revise policies
  - Revise procedures

Assist and Audit

- Provide on the spot (ad hoc) role-based information security training
- Assist in remediation of identified unacceptable risks
- Provide incident response capabilities and support
- Review program and system level information security for compliance and effectiveness
- Provide IHS ISSO office an avenue to interact with and promote coordination and cooperation with Area Facility personnel for P&P and standards efforts

Training and Awareness

- Collect data on information security training and awareness
- Develop and maintain an annual information security awareness course
- Develop and maintain a role-based information security training program
- Develop and maintain an information security training module in New Hire Orientation
- Provide periodic and ad hoc security awareness training and information security related news

Information Assurance and Standards Development

- Monitor antivirus and vulnerability notification sites
- Disseminate pertinent antivirus and vulnerability alerts
- Investigate mitigating recommendations for compatibility with IHS systems
- Verify recommended patches for compatibility with IHS systems and disseminate
- Maintain system inventories
- Track requirements compliancy such as C&A, PIA, risk assessments, and security plans
- Coordinate with and disseminate information from IDS services
- Develop, disseminate, and test compatibility with IHS systems, standard hardware and software configurations
- Evaluate C&A, FISMA POA&M, and IHS information security indicators and incorporate with operational and user needs to assess IHS information security posture, trends and requirements
- Investigate solutions for emerging information security requirements

Enterprise Integration

- Many of the activities for this function are determined by progress made at the IHS enterprise level with each of the areas listed below:
  - Strategic Planning
  - Enterprise Architecture
  - Capital Planning and Investment Control Program
  - Continuity of Operations Plan and Program
  - Managed Security Services Initiative
  - Other Enterprise Initiatives

INDIAN HEALTH SERVICE · DHHS · PHS

Metrics Development

- Define measurable and meaningful metrics
- Apply, track, collect, and report metrics
- Evaluate metrics and trends to make system and program improvement recommendations

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2004		
Assist and Audit 1 Contractor	Initiate A&A capability Initiate plans for dedicated Area Office ISSOs & ID funding	+ $150K
FY2005		
Assist and Audit 1 Position	Add to A&A capability and initiate IA&SD capability	+ $309K
Information Assurance & Standards Development 1 Position	Initiate plans for dedicated Area Office ISSOs & ID funding	

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2006		
Assist and Audit 2 Positions	Add to A&A, define two A&A teams	+ $2.39M
Information Assurance & Standards Development 1 Position	Initiate IHS Incident Response capability Add to IA&SD capability	
Information Security Support at Area Offices 12 Positions	Dedicated Area Office ISSOs at all Area Offices & ID funding	

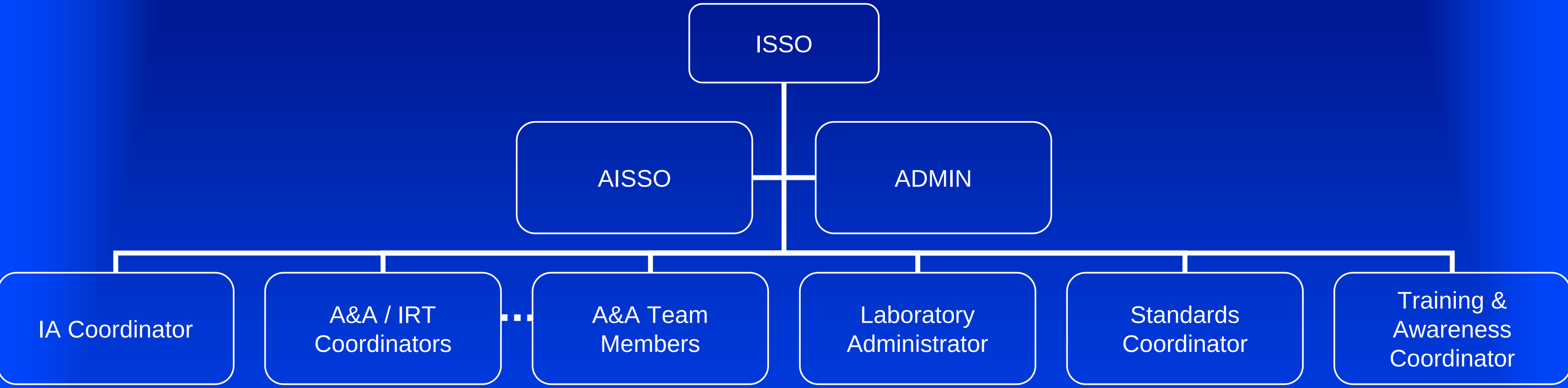
Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2007		
Assist and Audit 2 Positions	Add to A&A and IR capability	+ $492K
Training & Awareness 1 Position	Enhance T&A capability and initiate role-base training program & ID funding	
FY2008		
Assist and Audit 2 Positions	Complete two A&A and IR teams & ID funding	+ $338K

Proposed Timeline

Personnel	Planned Actions	Estimated Cost
FY2009		
	Evaluate capabilities and requirements – plan adjustments as necessary & ID funding	

Organization



ISSO

AISSO

ADMIN

IA Coordinator

A&A / IRT Coordinators

A&A Team Members

Laboratory Administrator

Standards Coordinator

Training & Awareness Coordinator

Staffing Source Options

- *Alternative A*
  - All federal employees (14)
- *Alternative B*
  - All federal employees (7) except; Assist Team members and Laboratory position, which would be contracted (7)
- *Alternative C*
  - All contractors (9) except; Assistant, Admin, Assist and Audit / Incident Response Team Coordinators, and Standards, which would be federal employees (5)
- *Alternative D*
  - All contractors (12) except; Assistant and Admin, which would be federal employees (2)

Discussion

Information Security Support Team Composition

- Information Assurance Coordinator (1 – GS 12/13)
- Assist and Audit / Incident Response Team Coordinator (2 – GS 13)
- Assist and Audit Team Member (6 – GS 11/12)
- Standards Coordinator (1 – GS 12/13)
- Laboratory Administrator (1 – GS 11/12)
- Training and Awareness Coordinator (1 – GS 11)
- Assistant (1 – GS 13)
- Administration Support (1 – GS 5)

Basic Duties and Responsibilities

- Information Assurance Coordinator – information security alerts / notifications, antivirus software, patch management, software configuration checks, web cookies, penetration and vulnerability testing, and IDS
- Assist and Audit / Incident Response Team Coordinator – IRT, Assist and Audit Team Coordinator, and lessons learned
- Assist and Audit Team Member – training and education, audit, remediation, network information maintenance
- Standards Coordinator – system configurations, hardware and software certification and accreditation, privacy impact, risk, and e-authentication assessments

Basic Duties and Responsibilities

- Laboratory Administrator – system administrator, IA, Assist and Audit Team support, and general support
- Training and Awareness Coordinator – training program definition, implementation, maintenance, and coordination, and awareness program maintenance
- Assistant – policies, procedures, and guidance maintenance, program metrics, requirements (i.e., Department, legislative, Administration) tracking, HIPAA, FISMA, COOP coordination, and program management / project officer functions
- Administrative Assistant – general administration

Team Mapped to IHS Policy

- Information Systems Security Officer. The IHS Information System Security Officer (ISSO) shall be responsible for the following:
  - Monitoring, evaluating, and reporting, as required, to the CIO on the status of ITS within the IHS and the adequacy of the ITS programs administered by the operating units. – accomplished via Assist and Audit Teams, Incident Response Teams, Assistant, and IA
  - Developing policies, procedures, and guidance establishing, implementing, maintaining, and overseeing requirements for the IHS's ITS program to be followed by all IHS organizations. – accomplished via Assistant, Assist and Audit Teams, Incident Response Teams, Laboratory, Standards, Training and Awareness, and IA
  - Providing guidance and technical assistance to operating units, including analyzing, evaluating, and approving all IT system security plans and requirements for IT systems security. – accomplished via Assistant, Assist Teams, Incident Response Teams, Laboratory, Standards, and IA

Team Mapped to IHS Policy

- Ensuring IHS ITS oversight through compliance reviews of operating units and organizations and ITS verification reviews of individual systems, and by participating in program management oversight processes. – accomplished via Assistant, Assist Teams, Incident Response Teams, Laboratory, Standards, and IA
- Maintaining a tracking system and records concerning implementation of the required controls and accreditation status of all IHS IT systems. – accomplished via Assistant, Assist Teams, Incident Response Teams, Laboratory, Standards, and IA
- Coordinating with Area ISSOs and periodically scheduling conference calls to discuss/disseminate information on ITS matters and concerns. – accomplished via Assistant
- Coordinating the review of controls and evaluating the adequacy of technical controls for accreditation. – accomplished via Assistant, IA, Assist Teams, Laboratory, and Standards

Team Mapped to IHS Policy

- Acting as the central point of contact for the Agency for ITS-related incidents or violations. – accomplished via Assistant and Incident Response Teams
- Investigating or initiating an investigation of any incidents or violations; maintaining records and preparing reports; disseminating information concerning potential threats; and reporting to the HHS senior ISSO any violations that come under his/her areas of responsibility or to the Assistant Inspector General for investigation any activity that may constitute a violation of law or otherwise is reportable to that office in accordance with District Attorney Order 207-10, "Inspector General Investigations.“ – accomplished via Assistant, Assist Teams, Incident Response Teams, and IA

Team Mapped to IHS Policy

- Coordinating information resources, security awareness, and training needs assessments; determining appropriate training resources; and coordinating training activities for target populations. (See HHS AISS Program Handbook Chapter VII, "Personnel Security/Suitability Training" and AIS-STOP. – accomplished via Assistant, Assist and Audit Teams, Incident Response Teams, Training and Awareness, and IA
- Assisting project officers and appropriate application system managers in carrying out the provisions of the HHS AISS Program Handbook for solicitations and contracts; and certifying the proposals received in response to a Request for Proposal (RFP) and certified as winning proposals by the Project Officer, as in the HHS AISS Program Handbook, Chapter XIV, "Acquisitions and Contracts." – accomplished via Assistant